REMARKS

In response to the Office Action mailed on March 11, 2008, Applicant respectfully requests reconsideration. Claims 1-5, 7-14, 17-21, 17-30, and 32-34 are now pending in this Application. Claims 1, 17, 30, and 32 are independent claims and the remaining claims are dependent claims. In this Amendment, claims 1, 7, 11, 17, 23, 30, and 32 have been amended. Claims 6 and 22 have been canceled. Applicant believes that the claims as presented are in condition for allowance. A notice to this affect is respectfully requested.

The Application was considered informal because the Abstract exceeded 150 words in length. Applicant amends the Abstract to cure this minor informality. The new Abstract which replaces the originally filed Abstract includes 150 words or less. Accordingly, the application should be considered as formal.

Amendments to the Claims

Claims 1, 7, 11, 17, 23, 30, and 32 have been amended. Independent claims 1, 30, and 32 have been amended to incorporate all of the limitations found in claim 6. Independent claim 17 has been amended to incorporate all of the limitations of claim 22. Claims 7, 11, and 23 were amended to correct claim dependencies necessitated by amendments to the independent claims. Thus, no new matter has been added to the claims which would justify a new ground of rejection.

Rejections under 35 U.S.C. § 101

The examiner rejects claim 1-5, 7-14, 17-21, 23-30, and 32 under 35 U.S.C. § 101. Applicant notes that claim one recites a method including: "identifying an incoming transmission including at least one identifiable portion; computing, for each identifiable portion in the incoming transmission, a fingerprint indicative of the at least one identified portion, the fingerprint being substantially unique to the at least one identified portion; and storing the computed fingerprint to generate a set of stored fingerprints; receiving a set of comparison fingerprints corresponding to a known portion of the incoming

transmission, the set of comparison fingerprints being predetermined; and comparing the set of stored fingerprints to the set of comparison fingerprints to identify stored fingerprints matching at least one of the set of comparison fingerprints and, if a match is found, identifying a previous incoming transmission corresponding to a matching stored fingerprint of the set of stored fingerprints; storing an indication of a subsequent disposition of the incoming transmission; receiving a subsequent set of comparison fingerprints, the subsequent set of comparison fingerprints indicative of refinements to the known portion of the incoming transmission; matching the subsequent set of comparison fingerprints to the stored fingerprints; determining, based on the matching of the subsequent set of comparison fingerprints, if the subsequent set of comparison fingerprints is indicative of an undesirable portion in the incoming transmission; and selectively performing, based on the determining, a remedial action in response to the subsequent disposition." Applicant traverses the rejection because the claimed invention is a statutory subject matter, and because the claimed invention produces both a useful and tangible result. For example, storing computed fingerprints is tangible. Also, storing a subsequent disposition of an incoming transmission is tangible. The limitation is useful because it identifies undesirable transmissions (such as a virus), and performs a remedial action in response. It is well-known that removing viruses from computers is useful. Thus, applicant respectfully requests that the rejection of claim 1 be withdrawn.

The examiner also rejects claims 17 and 32 under 35 U.S.C. § 101. Applicant notes that claim 17 recites that the invention is directed to a data communications device. A data communication device falls into multiple statutory categories: a patentable machine and a patentable manufacture. Moreover, the claims does positively recites a physical element is part of the device. More specifically, claim recites a processor. Any person of ordinary skill in the art would interpret this as a physical element.

The examiner also rejects claim 30 under 35 U.S.C. § 101. Applicant notes that claim 30 recites that the invention is directed to a computer program product having a computer readable medium. A computer program product is an article of manufacture

which is a physical, tangible object. Moreover, claims 17, 30, and 32 all contain the same useful and tangible result as that of claim 1.

The remaining claims rejected under 35 U.S.C. § 101 all depend from either claim 1 or claim 17, and thus recites statutory subject matter as well for the reasons discussed above. Applicant respectfully requests that the rejections under 35 U.S.C. § 101 be withdrawn.

Rejections under 35 U.S.C. §103

Claims 1-5, 7-14, 17-21, 23-30, and 32-34 have been rejected under 35 U.S.C. §103.

Claim 1. Claim 1, as amended, is equivalent to canceled claim 6. Claim 6 was rejected under 35 U.S.C. §103(a) is being unpatentable over Admitted Prior Art and common knowledge in the art, and further in view of Paul (USPN 6,052,709).

Conventional virus detection applications employ a set of known virus fingerprints for comparison. Fingerprints are for known viruses. Vendors provide periodic updates. Viruses have a period of largely unrestricted propagation pending detection and fingerprint generation.

Retroactive analysis and/or monitoring of previously excepted traffic is not included in the scope of protection. Conventional approaches do not maintain a propagation history or indication of successive dissemination.

As is apparent from the claim amendments, claim 1 claims a two part analysis. That is, in the context of virus detection, incoming transmissions are first scanned to see if there is a virus. Computed fingerprints from an incoming transmission are stored, at least temporarily, and matched with comparison fingerprints to identify undesirable transmissions. Those fingerprints of the incoming transmission are stored for subsequent analysis. After receiving an updated or subsequent set of virus definitions (set of comparison fingerprints), the previously processed transmissions are rematched to determine if any of the original incoming transmissions are identified as undesirable based on the updated set of comparison fingerprints. By storing a subsequent disposition of the incoming transmission, later discovered viruses can be remedied. In

other words, an incoming transmission is scanned a first time for a virus when the transmission is received, and then this same transmission is scanned a second time for a virus after receiving updated virus definitions. The second or subsequent VirusScan could be days, weeks, or months later.

Conventional virus detection applications are silent on storing an indication of the subsequent disposition of incoming transmissions, receiving a subsequent set of comparison fingerprints, matching the subsequent set of comparison fingerprints to the stored and previously-compared fingerprints, and identifying matches indicative of undesirable portions of the incoming transmission to selectively perform a remedial action.

The cited section of Paul does nothing more than describe a networked system for distributing spam filters. As new spam messages are discovered, spam definitions are updated across the network so the subsequent messages can be filtered with the updated spam messages. Paul, however, does not disclose re-filtering old messages with the subsequent spam definitions. Thus, Paul is nothing more than a spam filtering process that is equivalent to conventional virus detection processes.

The Paul reference is not relevant because once the filtering system is updated with new spam definitions existing e-mail is not re-filtered. Only subsequent e-mail messages are filtered, but stored e-mail messages are not re-filtered with subsequent spam definitions.

There is also no motivation to modify the Paul reference because there is no need to re-filter existing e-mail messages. Those designated as spam by a user are deleted at that time, thus there's no need to re-filter existing messages. Furthermore, unsolicited messages sitting in an e-mail box generally do not harm a computer. Viruses, however, can continue to harm a computer if not removed.

Thus, the reference combination fails to establish a prima facie case of obviousness. Claim 1 defines patentable subject matter, and is believed to be allowable.

Independent claims 17, 30, and 32, have been amended and now contain claim limitations that are substantially similar to claim 1. Therefore, claims 17, 30, and 32 are patentable over the reference combination for the reasons set forth above.

For applicable reasons as discussed above, each of dependent claims 2-5, 7-14, 18-21, and 23-29 are patentable over the reference combination.

Claims 33 and 34. Claims 33 and 34 were rejected under Admitted Prior Art, common knowledge in the art, and further in view of Van der Made (U.S. Pub. No. 20030212902). The cited paragraphs of Van der Made are [0037], [0013], and [0005] – [0007].

The Van der Made reference does not teach retroactive analysis in these paragraphs, nor is the term "retroactive" found anywhere in the Van der Made reference. The cited reference does not disclose identifying incoming transmissions, creating signatures of those transmissions, making an initial comparison to detect a virus, storing the transmission, receiving subsequent or updated fingerprints, and then performing a second comparison using the subsequent definition with the original transmission fingerprints, thereby performing a retroactive analysis.

According to Van der Made, A P-code is not analyzed for a virus twice, it is only analyzed once. The confusion comes from how each invention operates. The applicant's method uses signature/fingerprint matching to immediately identify a virus. Van der Made, however, operates by observing behavior and does not use a pattern matching approach. Instead, Van der Made creates virtual environments, or operating systems, in which a program runs and within which the process can observe behavior. The subsequent analysis, referred to in Van der Made, is not a secondary analysis of previously-analyzed transmission, but an analysis after all notes are taken during operation. In other words, the analysis is the first analysis of a program, subsequent to taking notes on program behavior.

Van der Made runs a program and then monitors, for example, decryption loops operating system calls, and read/write operations and set bits in a pattern register. These bits, by themselves, do not identify a malicious program, but such bits need to be

analyzed to identify behavior that is indicative of a virus. Thus there is no retroactive virus analysis disclosed in Van der Made — only a behavioral analysis after executing a program in a virtual environment.

Conclusion

In view of the foregoing remarks, applicant submits that the pending claims are in condition for allowance. A notice to this effect is respectfully requested. If the examiner believes, after reviewing this response, that the pending claims are not in condition for allowance, then the examiner is respectfully requested to call the representative.

Applicant hereby petitions for any extension of time that is required to maintain the pendency of this case. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-3735.

Respectfully submitted,

/joshuadmather/
Joshua D. Mather, Esq.
Attorney for Applicant(s)
Registration No.: 53,282
Chapin Intellectual Property Law, LLC
Westborough Office Park
1700 West Park Drive
Westborough, Massachusetts 01581
Telephone: (508) 616-9660
Facsimile: (508) 616-9661

Attorney Docket No.: SUN04-01(040577)

Dated: June 4, 2008